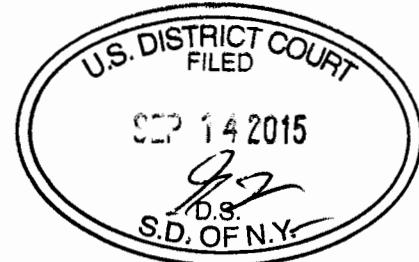


ORIGINAL

Approved: Kristy J. Greenberg
 Kristy J. Greenberg
 Assistant United States Attorney

Before: HONORABLE RONALD L. ELLIS
 United States Magistrate Judge
 Southern District of New York



15 MAG 3265

UNITED STATES OF AMERICA

- v. -

TIMOTHY SEDLAK,

Defendant.

AMENDED COMPLAINT

Violations of
 18 U.S.C. § 1030(b)

COUNTY OF OFFENSE:
 NEW YORK

SOUTHERN DISTRICT OF NEW YORK, ss.:

Erin Thackston, being duly sworn, deposes and says that she is a Special Agent with the United States Secret Service ("USSS") and charges as follows:

COUNT ONE
 (Computer Hacking)

1. From in or about June 2015, up to and including in or about July 2015, in the Southern District of New York and elsewhere, TIMOTHY SEDLAK, the defendant, would and did, and attempted to, intentionally access computers without authorization, and thereby would and did, and attempted to, obtain information from protected computers, for purposes of commercial advantage and private financial gain, and in furtherance of criminal and tortious acts in violation of the Constitution and the laws of the United States, in violation of Title 18, United States Code, Section 1030(a)(2), to wit, SEDLAK made hundreds of thousands of attempts to gain unauthorized access to computers of a specific global charitable organization's network in order to obtain information for his own commercial advantage and private financial gain.

(Title 18, United States Code, Section 1030(b).)

* * *

The bases for my knowledge and for the foregoing charges are, in part, as follows:

2. I have been a Special Agent with the USSS for approximately four years. I am currently assigned to the Electronic Crimes Task Force within the USSS's New York Field Office. I have been personally involved in the investigation of this matter. This affidavit is based upon my investigation, my conversations with other law enforcement agents, and my examination of reports, records, and other evidence. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

3. Based on my review of records of the and conversations with an employee of a global charitable organization with its principal office in New York, New York (the "Organization"), I have learned the following:

a. The Organization uses an Internet Service Provider's (the "First ISP") products for its business communications, including e-mail and other communications tools. Each employee of the Organization has a personal First ISP account (an "Account") that is connected to the Organization's network (the "Network"). The First ISP houses and manages a third-party service that combines its desktop suite with the First ISP's communications and collaboration services through the Internet, such as e-mail, internal social networking, collaboration, and a public web site, VoIP (voice over Internet Protocol) networks, Skype, and conferencing.

b. In order to access their Accounts, the Organization's employees are presented with a screen containing a prompt for a username and password. After entering a username and password, the Organization's employees are then permitted to access their Accounts, including their business e-mails, documents, and other communication tools. The Organization's computers are connected to the Internet.

c. From in or about June 2015, up to and including July 2015, numerous Organization employees reported that they had encountered difficulties accessing their Accounts. Specifically, Organization employees reported problems such as being locked out of their Accounts, and being redirected from

their Accounts after they had been initially accessed. As a result, numerous Organization employees, at least some of whom worked in the Organization's office in New York, New York, were disrupted in their ability to conduct regular business functions. These disruptions ceased when the Organization reset the configurations for the usernames of Organization employees, as well as asked Organization employees to reset their passwords.

d. The First ISP maintains logs of activity for the Accounts on the Organization's Network, and the Organization has direct access to that data. The logs include the date, time and IP Address associated with the access or attempted access of an Account, and the general location of the IP Address.¹ The logs document unsuccessful attempts to access the Accounts in which the correct username associated with the Account was entered by the user; however, the logs do not show unsuccessful attempts to access the Accounts in which the incorrect username and password was entered by the user.

e. Based on my review of the First ISP's log information for the Organization's Accounts, which I obtained from the Organization, I have learned the following:

i. Between June 22, 2015 and July 8, 2015, there were approximately 195,000 unsuccessful attempts by an IP address ("the First IP Address") to log on to approximately twenty of the Organization's Accounts, at least some of which belonged to employees who worked and used computers in the Organization's office in New York, New York.

ii. Between July 8, 2015 and July 10, 2015, there were approximately 195,000 unsuccessful attempts by

¹ The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses. A device's IP address can be used to determine its physical location and, thereby, its user.

another IP address (the "Second IP Address") to log on to approximately six of the Organization's Accounts.

f. TIMOTHY SEDLAK, the defendant, has never been employed by the Organization, and has not been authorized to access any Accounts of the Organization.

4. Based on my training and experience, and my review of the activity history of Accounts of the Organization, the hundreds of thousands of unsuccessful attempts to access the Organization's Accounts are well in excess of the typical number, and are consistent with an attempt to gain unauthorized access to the Accounts of the Organization.

5. Based on information obtained pursuant to a grand jury subpoena from another Internet Service Provider (the "Second ISP"), I have learned the following:

a. The subscriber for the Second ISP account identified with both the First IP Address and the Second IP Address is listed as "Timothy Sedlak" at a particular residence in Ocoee, Florida (the "Sedlak Residence").

b. The First IP Address began to be used on June 13, 2015, shortly before the attempts to unlawfully access Accounts at the Organization commenced, and is identified with an electronic device containing a particular media access control address (the "MAC Address")² and a particular e-mail account incorporating the first and last name of Tim Sedlak (the "Sedlak E-mail Account").

c. The Second IP Address was used on July 8-10, 2015, and is also associated with a device containing the MAC Address and the Sedlak E-mail Account.

6. Based on my review of documents obtained from the Florida Department of Motor Vehicles, I have learned that the "Sedlak Residence" is currently listed as the address on the driver's license of TIMOTHY SEDLAK, the defendant.

7. Based on my review of a LinkedIn account for "Timothy Sedlak," I learned that "Timothy Sedlak" is listed as an

² A media access control address is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most network technologies, including Ethernet and Wi-Fi.

investigator with a particular company (the "Company") in Orlando, Florida.

8. Based on my review of information from the Florida Department of Agriculture, I have learned that in order to work as a private investigator, one must be licensed, and that TIMOTHY SEDLAK, the defendant, currently does not have a license to work as a private investigator in the state of Florida.

9. From my personal participation in this investigation, as well as from speaking with other law enforcement officers, I have learned the following:

a. On or about September 11, 2015, USSS agents and I executed a search warrant at the Sedlak Residence. The agents located at the Sedlak Residence and seized, among other things, the following:

i. Approximately 30 computers connected to the same internal network, which enabled each computer to communicate with the others (the "Sedlak Computers");

ii. Notes pertaining to the Organization, an executive of the Organization ("Individual-1") and an individual who has been publicly affiliated with the Organization ("Individual-2"), including e-mail addresses, registrant information for certain website domain names, and certain IP address information associated with the Organization, Individual-1 and/or Individual-2; and

iii. Documents containing lists of e-mail addresses with their corresponding e-mail servers,³ which contained words such as "jihad." Based on my training and experience, these documents indicate an attempt to hack into e-mail servers.

b. Pursuant to the search warrant, I have conducted a preliminary review of computers seized from the Sedlak Residence. From this review, I have learned:

i. There is a list of usernames for Organization Accounts in certain of the Sedlak Computers; and

³ Based on my training and experience, I know that an e-mail server is a high-capacity computing device that runs software dedicated to sending, delivery and storage of e-mail messages.

ii. There is a brute force password cracking tool in certain of the Sedlak Computers. Based on my training and experience, I know that a brute force password cracking tool is designed to guess passwords from databases that have been stored in or are in transit within a computer system or network. Brute Force means that the program launches a relentless barrage of passwords at a log in to guess the password utilizing a password list compiled by the hacker. Brute force will take the list that the hacker built and will likely combine it with other common passwords, and then begin the attack. Depending on the processing speed of the hacker's computer and Internet connection, the brute force methodology will systematically go through each password until the correct one is discovered.

c. Based on my training and experience, the number of computers in the Sedlak Residence and the manner in which they were networked together is consistent with an attempt to gain unauthorized access to computers, as well as a plan to engage in distributed denial of service ("DDos") attacks. A denial of service ("DoS") attack is a type of attack on a network that is designed to disrupt the network by flooding it with useless traffic. A distributed denial of service ("DDoS") attack is a type of denial of service attack where multiple compromised systems, which are often infected with a Trojan (i.e., a destructive program that masquerades as a benign application), are used to target a single system causing a Dos attack.

d. Another USSS agent ("Agent-1") and I interviewed TIMOTHY SEDLAK, the defendant, who voluntarily agreed to answer questions, in the Sedlak Residence. SEDLAK told Agent-1 and me, in sum and substance, and in part, the following:

i. That his name is Timothy Sedlak, and that he resides alone at the Sedlak Residence;

ii. That all the computers in the Sedlak Residence belong to him, and that he exclusively uses them. He taught himself how to set those computers up on the Internet. His computers are connected to the Internet, but he does not have Wi-Fi, so no one else can use his network connection to access the Internet;⁴

⁴ Based on my training and experience, I know that Wi-Fi is a wireless local area network that enables a device to connect to the Internet. Wi-Fi can be less secure than wired connections,

iii. That he has conducted "research" of charitable organizations to try to determine if such organizations are unintentionally financing jihadist groups by sending, to charitable organizations in the Middle East, funds which are then seized by jihadist groups;

iv. When asked about notes pertaining to Individual-1 and Individual-2 found at the Sedlak Residence, he claimed that he came across such information in his "research" into the financing of jihadist groups;

v. That he has conducted this "research" into charitable organizations in the course of his work as a private investigator, and hoped to sell the information he found;

vi. That he has been paid by clients to work as a private investigator, but that he cannot discuss the work he has done for them; and

vii. When I asked him whether he attempted to hack the computers of any charitable organizations, he stated that he could not talk about it because it was part of his work.

10. After speaking with Agent-1 and me, TIMOTHY SEDLAK, the defendant, was arrested at the Sedlak Residence.

such as Ethernet, precisely because an intruder does not need a physical connection.

WHEREFORE, I respectfully request that an arrest warrant be issued for TIMOTHY SEDLAK, the defendant, and that he be arrested and imprisoned or bailed, as the case may be.


Erin Thackston
Special Agent
United States Secret Service

Sworn to before me this
14th day of September 2015


HON. RONALD L. ELLIS
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK